DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents
May 30 - July 3, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000063116	Mishandled/ Misused Physical or Verbal Information	VISN 07 Columbia, SC	5/31/2011	6/13/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	5/31/2011	INC000000152806	N/A	N/A	N/A		1

Incident Summary

A pharmacy package was delivered to the wrong individual. The Veteran no longer resides at the address where the package was delivered. The individual contacted Pharmacy Service staff regarding the misdirected package. The individual who received the package is not a Veteran. The individual has the same last name as the Veteran. The information disclosed included an instruction sheet which included the Veteran's full name, name of medication, dosage, and an incorrect address. The UPS and VA Police have been notified. A pharmacist attempted to contact the Veteran by phone, but the phone had been disconnected. UPS has been contacted to arrange for a pick-up of the package.

Incident Update

05/31/11:
The Veteran will be sent a notification letter due to name and protected health information (PHI) being exposed.

NOTE: There were a total of 90 Mis-Mailed incidents this reporting period. Because of repetition, the other 89 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

Employees are being re-educated on the need to safeguard patient information, and the importance of being vigilant when disbursing medication via the pharmacy window as well as through the mail.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000063135	Mishandled/ Misused Physical or Verbal Information	VISN 06 Beckley, WV	5/31/2011	7/7/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	5/31/2011	INC000000152915	N/A	N/A	N/A		1

Incident Summary

A Pharmacy technician inadvertently gave Patient A's prescription and accompanying paperwork to Patient B. The Pharmacy technician realized the mistake and the Chief of Pharmacy contacted Patient B. Patient B confirmed he has Patient A's prescription and accompany paperwork and is in the process of returning it now. The prescription bottle label contains Patient A's name and name of medication. The accompanying paperwork has Patient A's name on it and Patient A's address. No other personal information was disclosed.

Incident Update

05/31/11:
Patient A will be sent a notification letter due to full name and medication type being exposed.

NOTE: There were a total of 68 Mis-Handling incidents this reporting period. Because of repetition, the other 67 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The Chief of Pharmacy has reviewed their procedures and has provided additional training to the technician who dispensed the medication.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000063253	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	6/3/2011	6/29/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	6/3/2011	INC000000153558	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

06/03/11:
Patient B will be sent a notification letter.

NOTE: There were a total of 5 Mis-Mailed CMOP incidents out 7,509,100 total packages (10,936,341 total prescriptions) mailed out for this reporting period. Because of repetition, the other 4 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The CMOP employee was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000063370	Missing/Stolen Equipment	VISN 23 Iowa City, IA	6/7/2011	6/27/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	6/7/2011	INC000000154079	N/A	N/A	N/A		

Incident Summary

During a routine Bio-Medical Inventory, it was noted a VA laptop and VA workstation could not be located. Both items were older equipment that was moved from the OIT Operating inventory and transferred to the Bio-Medical inventory, refurbished and used as Bio-Medical device equipment. The original hard drives which may have contained Personally Identifiable Information (PII) or Protected Health Information (PHI) had been removed, turned in for destruction and replaced with new hard drives for Bio-Medical use only. The non-encrypted laptop and workstation are Bio-Medical workstations used only to diagnose medical equipment and did not contain PII or PHI. The equipment still may be located in the Medical Center. The VA Police and Logistics have been notified and the Report of Survey process has been initiated.

Incident Update

NOTE: There were a total of 8 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 7 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

There is no data breach. No PII or PHI is stored on the equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000063670	Mishandled/ Misused Physical or Verbal Information	VISN 11 Detroit, MI	6/14/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	6/14/2011	INC000000155519	N/A	N/A	N/A	10049	66

Incident Summary

On the second day of an Information Technology Oversight and Compliance (ITOC) inspection, the ITOC inspector requested to see the hard copy, wet signature Rules of Behavior (ROB) forms on 5 employee/contractors to see if the documentation was on file. Two of the five requested forms were found. Office of Information and Technology (OIT) staff were requested to pull the ROBs since they were stored there. The following day the ISO was informed that OIT no longer had the books because the binders were tossed out during a move. The binders were clearly labeled chronologically and alphabetically. The ISO asked the OIT staff to look everywhere in case they were misplaced during the move from the 7th floor back to the basement. The OIT staff looked for the documents all over the department for 4 days. One of the OIT employees stated that the binders were tossed in the trash during the move from the 7th floor. This incident happened almost a year ago, was only discovered several days ago, and confirmed on 06/14/11. The documents thrown out included all of the computer access forms from the beginning of the VISTA computer system through 2005. Also thrown out were documents of VISTA patches and VISTA programs.

Incident Update

06/15/11:
The ISO requested that OIT pull a VISTA report of VISTA employees from Feb 1987 through Dec 31, 2005. When completed, the ISO will send the total number of employees to the NSOC. The personally identifiable information (PII) included on the computer access forms were full name, date of birth and full SSN. Beginning in 2007 when OMB instructed all Federal Agencies to remove the full SSN, the access forms were changed to include the last four of the SSN instead of the full SSN.

06/23/11:
After removing duplicates, the number of affected individuals stands at 18,557. All of these had at least full name and date of birth on the forms. Some also included full SSNs. IT staff are continuing an extensive search of the facility in order to be certain the binders are missing.

06/28/11:
The national Data Breach Core Team (DBCT) decided that credit protection services/next of kin notifications will need to be done for all employees on the list. After removal of additional duplicates, the final number that has been accounted for in the report is 10,115 users.

07/05/11:
The most recent review of the list of employees indicates that 66 are deceased and will require next of kin notification.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064167	Missing/Stolen Equipment	VISN 09 Nashville, TN	6/27/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	6/27/2011	INC000000157805	N/A	N/A	N/A		

Incident Summary

In November 2010, the Prosthetics & Sensory Aids Service moved to a temporary location to have the service area renovated. A Hewlett Packard laptop that is used to assist in making prosthetic limbs was locked in a black 4 foot storage cabinet with some other items that were supposed to go to VA Storage until the renovation was completed. The laptop was not among the items that were returned to the service from storage. The person reporting the missing laptop stated that only patient names, weights, and heights were stored on this equipment.

Incident Update

06/28/11:
The laptop was not encrypted. It was purchased by the Bio-Medical Service as support for making prostheses and it was never on the VA network. The patient data on the laptop was less than 30 patient names, heights, and weights. There was no SSN, date of birth, or diagnosis. The laptop uses proprietary software. There is not enough information stored on the laptop that would require notification to the individuals.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064294	Missing/Stolen Equipment	VISN 19 Salt Lake City, UT	6/29/2011	7/1/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	6/29/2011	INC000000158312	N/A	N/A	N/A		

Incident Summary

A laptop used to monitor a piece of research analysis equipment has been reported missing. This device was not connected to the VA network and did not contain any personally identifiable information (PII) or protected health information (PHI).

Incident Update

06/30/11:
The Information Security Officer (ISO) reports that there was no reason to encrypt the laptop as it contained no PII or PHI and was connected to a research analysis device which was used for animal studies.

Resolution

The Research Service employees have been reminded regarding the physical security of VA equipment. The investigation will continue to see if the laptop can be found.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064370	Mishandled/ Misused Physical or Verbal Information	VISN 19 Denver, CO	7/1/2011		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/1/2011	INC000000158728	N/A	N/A	N/A	58	

Incident Summary

VA Police conducted a foot patrol around the medical center during off business hours and found unsecured printed documents containing individually identifiable information.

Incident Update

07/01/11:
The papers were routing slips that had 58 Veterans' full SSN on them. The 58 Veterans will receive a letter offering credit protection services.

Resolution

The Privacy Office recommends education on reasonable safeguard practices for the employees who work in this area. Employees were reminded to lock up documents containing personally identifiable information (PII) or protected health information (PHI) after their shift.

Total number of Lost Blackberry Incidents	23
Total number of Internal Un-encrypted E-mail Incidents	93
Total number of Mis-Handling Incidents	68
Total number of Mis-Mailed Incidents	90
Total number of Mis-Mailed CMOP Incidents	5
Total number of IT Equipment Inventory Incidents	8
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	18 (15 encrypted)